UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/595,019	12/16/2005	Johnson Oyama	P18387US2	1263

27045 7590 04/14/2010

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
PHAM, LUU T	

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
04/14/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

melissa.wingo@ericsson.com
kara.coffman@ericsson.com
jennifer.hardin@ericsson.com

Office Action Summary	Application No.	Applicant(s)	
	10/595,019	OYAMA, JOHNSON	
	Examiner	Art Unit	
	LUU PHAM	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 March 2010 and 29 December 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *4,8-14,16-19,22,31-37,39-41,51 and 52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *4,8-14,16-19,22,31-37,39-41,51 and 52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the Amendment filed on 03/17/2010 and 12/29/2009.

2. In the instant Amendment, Claims 1-3, 5-7, 15, 20-21, 23-30, 38, and 42-50 were previously canceled; Claims 51 and 52 are independent claims. Claims 4, 8-14, 16-19, 22, 31-37, 39-41, and 51-52 have been examined and are pending.

   This Action is made FINAL.

Response to Arguments

3. As requested by the Applicants, a telephone interview with the Examiner and his SPE was held on April 08. During the telephone interview claim rejections under 35 U.S.C. 112, first paragraph and 35 U.S.C. 102(e) were discussed. The Examiner pointed out that although the claimed invention a concept of *'mere pass-through agent(s),'* the specification and claim language do not clearly define functions and/or actions of mere pass-though agent(s). If the claim recites *"without modify encrypted authentication information"* or *"without analysis authentication information,"* then Faccin reference encompasses all limitations claimed because Faccin reference does not modify/analysis encrypted information at all. The Examiner suggested that the claim be further amended to clearly define functions/actions of *'mere pass-through'* of the AAA Client and/or AAAv to distinguish the claimed invention over prior art of record. The Applicant considers dropping limitations rejected under 35 U.S.C. 112, 1st paragraph, and will further amend the claim to clarify the claimed invention.

4. The objection to the specification is maintained as the specification fails to provide proper antecedent basis for the claimed subject matter.

5. The rejections of claims 4, 8-14, 16-19, 22, 31-37, 39-41, and 51-52 under 35 U.S.C. § 112, first paragraph, are maintained. Applicants' arguments with respect to the support for limitations recited in claims 51-52 *(pages 1-2, section 3 of the Remarks, submitted on 12/29/2009)* have been fully considered but they are not persuasive.

Applicants' arguments:

> *"Support for theses steps is found at least in the following locations in the specification: Page 3, lines 1-7; Page 3, lines 19-24; Page 3, lines 28 through page 4, line 8; Page 4, lines 10-15; Page 4, lines 21-30; ..."*

The Examiner disagrees for the following reasons

> After having carefully reviewed the specification, the Examiner respectfully submits that no where does the specification disclose *"**encrypting authentication and authorized information in a mobile node**," "sending the **encrypted authentication and information**," "forwarding the **encrypted authentication and information**,"* and *"performing an **analysis of the encrypted authentication and authorized information;**"* (emphasis added). At most, in page 3, lines 23-25, the Applicants discuss *"other objects are to provide a mechanism for MIPv6 support that is complete as well as transparent to the visited domain;"* in page 6, lines 21-23, the Applicants discuss *"[w]ith such a solution it is not possible to apply prior encryption between MN and AAAh and the exchanges are visible over the air interface;"* and page 7, lines 17-18, the Applicants discuss *"[i]t will also be possible to apply prior*

encryption between MN and AAAh." However, the above discussions do not fully support the claimed limitations *"**encrypting authentication and authorized information in a mobile node**," "sending the **encrypted authentication and information**," "forwarding the **encrypted authentication and information**,"* and *"performing an **analysis of the encrypted authentication and authorized information;**"* (emphasis added). The Examiner respectfully requests the Applicant particularly point out where in the specification support can be found for the aforementioned newly added limitations. The Examiner also suggests that the claim be further amended to clearly describe the 'mere pass-through' functions of the AAA Client and/or AAAv to distinguish the claimed invention over prior art of record.

6. Applicants' arguments in the instant Amendment, filed on 12/29/2009, with respect to 35 U.S.C. 102 and 35 U.S.C. 103 rejections have been fully considered but they are not persuasive.

Applicants' arguments:

a. *"[T]he visited domain decrypts the return message from the home AAA server as noted in paragraph 0067. Thus, the visited domain is not acting merely as pass-through agent."*

b. "*Faccin '884 expressly teaches away from the claimed invention by stating that the visited domain decrypts messages sent from the home AAA server to the mobile node.*"

The Examiner disagrees for the following reasons:

a. As described in paragraphs [0065]-[0066], mobile node sends message 208 *[CK,IK(DH_MN), RAND_VD]* to visited domain 202. The visited domain 202 can not decrypt the encrypted message *CK,IK(DH_MN)* as it can not compute key Kc. The visited domain forms message 210 *[CK,IK(DH_MN), K1(DH_VD)]* by appending encrypted portion K1(DH_VD), wherein DH_VD is the encrypted using key K1, with the encrypted message *[CK,IK(DH_MN)]* received from the mobile node. The visited domain then sends the message 210 *[CK,IK(DH_MN), K1(DH_VD)]* to home domain 204. It is clear that the visited domain 202 does **'pass' the encrypted message *CK,IK(DH_MN)* to the home domain 204;** (emphasis added). Because the visited domain 202 can not decrypt the encrypted message *CK,IK(DH_MN)*, that means the visited domain 202 does not analyze the encrypted message CK,IK(DH_MN) at al. Therefore, Faccin '884 encompasses all limitations in argued in claims 51 and 52. In addition to the above, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *"the visited domain is not acting merely as a pass-through agent"*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The Examiner respectfully suggests that the claim be further amended to clearly

describe the 'mere pass-through' functions of the AAA Client and/or AAAv to distinguish the claimed invention over prior art of record.

b. It would be fallacious to conclude that *"Faccin '884 expressly 'teach away' from the claimed invention,"* since nowhere does Faccin '884 criticize, discredit, or otherwise discourage the solution comprising *"forwarding the encrypted authentication and authorization information from the AAA client to a visited AAA server in the visited network without analyzing the encrypted authentication and authorization information by the AAA client"* and *"forwarding the encrypted authentication and authorization information from the visited AAA server in the visited network to a home AAA server in the mobile node's home network without analyzing the encrypted authentication and authorization information by the visited AAA server,"* as claimed by the Applicant. *"The prior art's mere disclosure of more than one alternative does not constitute a teaching away from any of these alternatives because such disclosure does not criticize, discredit, or otherwise discourage the solution claimed...."* In re Fulton, 391 F.3d 1195, 1201, 73 USPQ2d 1141, 1146 (Fed. Cir. 2004). See also MPEP §2123. Therefore, the references do not teach away from the claimed invention. As a result, combing Faccin '844 and Faccin_Internet-Draft and Faccin '884 and Akhtar are proper.

Specification

7. The Specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required. Newly added claims, claims 51 and 52, recite limitations *"**encrypting authentication and authorized information in a mobile node**," "sending the **encrypted authentication and information**," "forwarding the **encrypted authentication and information**,"* and *"performing an **analysis of the encrypted authentication and authorized information.**"* (emphasis added). However, the aforementioned limitations are not found in the Specification. There is insufficient antecedent basis for said newly added limitations.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. **Claims 4, 8-14, 16-19, 22, 31-37, 39-41, and 51-52**, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

- **Regarding claims 51 and 52**; newly added claims, claims 51 and 52, recite limitations *"**encrypting authentication and authorized information in a mobile node**,"* *"sending the **encrypted authentication and information**,"* *"forwarding the **encrypted authentication and information**,"* and *"performing an **analysis of the encrypted authentication and authorized information**,"* (emphasis added). However, the aforementioned limitations are not discussed in the specification. Although the Applicant points out *"[t]he amendment is supported in the specification on page 4, lines 21-30,"* the discussions in page 4, wherein *"the proposed MIPv6 authentication/authorization solution is transparent to the visited domain, which is one of the major advantages of using a protocol like EAP. This makes it possible to apply prior encryption between MN and AAAh,"* are not sufficient support the newly added limitations as mentioned above. Nowhere does the specification discuss or suggest steps of *"encrypting authentication and authorized information in a mobile node,"* *"sending the encrypted authentication and information,"* *"forwarding the encrypted authentication and information,"* and *"performing an analysis of the encrypted authentication and authorized information."* The Examiner respectfully requests the Applicant point out where in the specification support can be found for the aforementioned newly added limitations. Applicant is required to cancel the new matter in the reply to this Office Action.

- **Regarding claims 4, 8-14, 16-19, 22, 31-37, and 39-41**; claims 4, 8-14, 16-19, 22, 31-37, 39-41 are dependent on either claim 51 or claims 52, and therefore inherit the 35 U.S.C 112, first paragraph issues of the independent claims.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. **Claims 4, 16-17, 19, 39-40, and 51-52 are rejected under 35 U.S.C. 102(e)** as being anticipated by Faccin et al., (hereinafter "Faccin '844"), U.S. Patent Application Publication No. 2002/0120844, filed on February 23, 2001.

- **Regarding claim 4**, Faccin '844 discloses the method of claim 51, further comprising transferring MIPv6-related information from the AAA server in the home network to a home agent *(pars. 0092-0100; Figs. 3-5; AAA-H/AuC 312 sends Km to HA 314)*.

- **Regarding claim 16**, Faccin '844 discloses the method of claim 4, wherein the MIPv6- related information is transferred from the AAA server in the home network to the home agent in an AAA framework protocol application *(pars. 0092-0100; Figs. 3-5; the AAA-H/AuC 312 then chooses a Home Agent and sends the Mobile IP key Km to the selected HA)*.

- **Regarding claim 17**, Faccin '844 discloses the method of claim 16, wherein the home agent is a local home agent in the visited network and the MIPv6-related information is transferred from the AAA home server to the local home agent via an AAA server in the visited network *(pars. 0111-0112; Fig. 5; wherein at least step 522)*.

- **Regarding claim 19**, Faccin '844 discloses the method of claim 4, further comprising:

assigning, by the home AAA server, a home agent to the mobile node *(pars. 0052, 0058-0059, and 0100; The AA-H/AuC 106 then chooses a home agent for the mobile node 100, and sends Mobile IP Key Km to the chosen home agent 108)*; and

distributing by the home AAA server to the mobile node and the home agent, credential-related data for establishing a security association between the mobile node and the home agent *(0052, 0058-0059, and 0100; The AA-H/AuC 106 then chooses a home agent for the mobile node 100, and sends Mobile IP Key Km to the chosen home agent 108)*.

- **Regarding claims 39-40**, claims 39-40 are similar in scope to claims 16-17 respectively, and are therefore rejected under similar rationale.

- **Regarding claim 51**, Faccin '844 discloses a method of authentication and authorization support for Mobile IP version 6 (MIPv6) *(pars. 0002 and 0011-0013)*, comprising the steps of:

encrypting authentication and authorization information in a mobile node operating in a visited network *(pars. 0030, 0038, 0065, and 0089-0091; Figs. 2 and 3, step*

208; MN 200 sends its DH value, encrypted with CK and integrity protected with IK, i.e. CK, IK (DH_ MN));

sending the encrypted authentication and authorization information from the mobile node to a pass-through Authentication, Authorization and Accounting (AAA) client in the visited network utilizing a protocol for carrying authentication information for network access *(par. 0065; Fig. 2, step 208; the Visited Domain 202 receives the first message but cannot decrypt it since it does not know how to compute Kc, and transmits it to the home domain 204; 'CK,IK(DH_MN)' is known as encrypted authentication and authorization information; pars. 0089-0092; Fig. 3, steps 328-332; the BU is forwarded to the AAA-H)*;

forwarding the encrypted authentication and authorization information from the AAA client to a visited AAA server in the visited network without analyzing the encrypted authentication and authorization information by the AAA client *(par. 0065; Fig. 2, step 208; the Visited Domain 202 receives the first message but cannot decrypt it since it does not know how to compute Kc, and transmits it to the home domain 204; pars. 0089-0092; Fig. 3, steps 318 and 330; Fig. 4, steps 418 and 422; the BU is forwarded to the AAA-H)*;

forwarding the encrypted authentication and authorization information from the visited AAA server in the visited network to a home AAA server in the mobile node's home network without analyzing the encrypted authentication and authorization information by the visited AAA server *(par. 0065; Fig. 2, step 210; the Visited Domain 202 receives the first message but cannot decrypt it since it does not know how to compute Kc, and transmits it to the home domain 204; pars. 0089-0092; Figs. 3 and 4, steps 320*

and 332; the BU is forwarded to the AAA-H; the AAA-H/AuC 312 verifies the MAC value to make sure the message has not been modified);

performing an analysis of the encrypted authentication and authorization information by the home AAA server *(pars. 0066 and 0092-0101; Figs. 3-4; The AAA-H/AuC 312 verifies the MAC value to make sure the message has not been modified)*;

sending a MIPv6-related challenge message from the home AAA server to the mobile node via the visited AAA server and the pass-through AAA client in the visited network based on the analysis of the encrypted authentication and authorization information, wherein the visited AAA server and the AAA client forward the challenge message without analyzing the challenge message contents *(pars. 0068-0069; Fig. 2, steps 212 and 214; the visited domain forwards a message 214 comprising the visited domain DH value encrypted with key CK and integrity protected by IK, compiled by the home domain 201, to the mobile node 200; 'CK,IK(DH_VD)' is considered as 'challenge message contents' since MN, which is the only communication node, is able to decrypt it; see also Fig. 5, steps 522-532)*;

sending a MIPv6-related challenge response message from the mobile node to the home AAA server via the AAA client and the visited AAA server in the visited network, wherein the AAA client and the visited AAA server forward the challenge response message without analyzing the challenge response message contents *(pars. 0106 and 0108-0112; Fig. 3, steps 352-354; the MN executes a BU with its HA; Fig. 4, step 424; Fig. 5, steps 521-522; the third BU (arrows 424, 426) is a BU with the MN's Home Agent: the AR cannot perform this BU because it does not have the Mobile IP Key; see also par. 0065; Fig. 2, step 208; the Visited Domain 202 receives the first message but cannot*

decrypt it since it does not know how to compute Kc, and transmits it to the home domain 204; 'CK,IK(DH_MN)' is known as challenge response message contents since home server, which is the only communication node, is able to decrypt it);

performing an analysis of the challenge response message contents by the home AAA server *(pars. 0066-0068, 0092-0096, and 0106-0112; Figs. 3-5, the Home network performs authentication the user; the third BU (arrows 424, 426) is a BU with the MN's Home Agent; the AR cannot perform this BU because it does not have the Mobile IP Key)*; and

sending a MIPv6-related authentication and authorization results message from the home AAA server to the mobile node reporting a result of the analysis of the challenge response message contents and providing session parameter information *(pars. 0092-0096, 0106-0112; Figs. 3-5; steps 354, 426, and 532; the MN executes a BU with its HA)*.

- **Regarding claim 52**, Faccin '844 discloses a system for authentication and authorization support for MIPv6 *(pars. 0002 and 0011-0013)*, comprising:

a mobile node operating in a visited network for encrypting authentication and authorization information and for sending the encrypted authentication and authorization information from the mobile node to a pass-through Authentication, Authorization and Accounting (AAA) node in the visited network utilizing a protocol for carrying authentication information for network access *(pars. 0030, 0038, 0065, and 0089-0091; Figs. 2 and 3, step 208; MN 200 sends its DH value, encrypted with CK and integrity protected with IK, i.e. CK, IK (DH_ MN); par. 0065; Fig. 2, step 208; the Visited Domain 202 receives the first message but cannot decrypt it since it does not know how to compute*

Kc, and transmits it to the home domain 204; 'CK,IK(DH_MN)' is known as encrypted authentication and authorization information; pars. 0089-0092; Fig. 3, steps 328-332; the BU is forwarded to the AAA-H);

the pass-through AAA node for forwarding the encrypted authentication and authorization information to a home AAA server in the mobile node's home network without analyzing the encrypted authentication and authorization information *(par. 0065; Fig. 2, step 210; the Visited Domain 202 receives the first message but cannot decrypt it since it does not know how to compute Kc, and transmits it to the home domain 204; pars. 0089-0092; Figs. 3 and 4, steps 320 and 332; the BU is forwarded to the AAA-H; the AAA-H/AuC 312 verifies the MAC value to make sure the message has not been modified)*;

the home AAA server for performing an analysis of the encrypted authentication and authorization information *(pars. 0066 and 0092-0101; Figs. 3-4; The AAA-H/AuC 312 verifies the MAC value to make sure the message has not been modified)* and for sending a MIPv6-related challenge message to the mobile node via the pass-through AAA node in the visited network based on the analysis of the encrypted authentication and authorization information, wherein the pass-through AAA node forwards the challenge message without analyzing the challenge message contents *(pars. 0068-0069; Fig. 2, steps 212 and 214; the visited domain forwards a message 214 comprising the visited domain DH value encrypted with key CK and integrity protected by IK, compiled by the home domain 201, to the mobile node 200; 'CK,IK(DH_VD)' is considered as 'challenge message contents' since MN, which is the only communication node, is able to decrypt it; see also Fig. 5, steps 522-532)*;

wherein the mobile node sends a MIPv6-related challenge response message to the home AAA server via the pass-through AAA node in the visited network, wherein the

pass-through AAA node forwards the challenge response message without analyzing the challenge response message contents *(pars. 0106 and 0108-0112; Fig. 3, steps 352-354; the MN executes a BU with its HA; Fig. 4, step 424; Fig. 5, steps 521-522; the third BU (arrows 424, 426) is a BU with the MN's Home Agent: the AR cannot perform this BU because it does not have the Mobile IP Key; see also par. 0065; Fig. 2, step 208; the Visited Domain 202 receives the first message but cannot decrypt it since it does not know how to compute Kc, and transmits it to the home domain 204; 'CK,IK(DH_MN)' is known as challenge response message contents since home server, which is the only communication node, is able to decrypt it)*; and

wherein the home AAA server performs an analysis of the challenge response message contents by the home AAA server (pars. 0066-0068, 0092-0096, and 0106-0112; Figs. 3-5, the Home network performs authentication the user; the third BU (arrows 424, 426) is a BU with the MN's Home Agent; the AR cannot perform this BU because it does not have the Mobile IP Key), and sends a MIPv6-related authentication and authorization results message to the mobile node reporting a result of the analysis of the challenge response message contents and providing session parameter information (pars. 0092-0096, 0106-0112; Figs. 3-5; steps 354, 426, and 532; the MN executes a BU with its HA).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

14. **Claims 8-10, 12-14, 22, 31-33, and 35-37 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Faccin, as applied to claims 51 and 52 above, in view of Faccin et al., (hereinafter "Faccin_Internet-Draft"), "Diameter Mobile IPv6 Application, draft-le-aaa-diameter-mobileipv6-6-03.txt," Internet Draft, XP015004098, published in April 2003.

- **Regarding claim 8**, Faccin '844 discloses the method of claim 51.

Faccin '844 does not explicitly discloses the protocol for carrying authentication information for network access is an extended Extensible Authentication Protocol (EAP)

and the MIPv6-related challenge and response messages are incorporated as additional data in the EAP protocol stack.

However, in an analogous art, Faccin_Internet-Draft discloses a Mobile IPv6 document, wherein the protocol for carrying authentication information for network access is an extended Extensible Authentication Protocol (EAP) and the MIPv6-related challenge and response messages are incorporated as additional data in the EAP protocol stack *(Faccin_Internet-Draft: page 5, section 4.1; page 10, section 6.2; pages 22-24; sections 9.3-9.5)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Faccin_Internet-Draft with the method and system of Faccin wherein the protocol for carrying authentication information for network access is an extended Extensible Authentication Protocol (EAP) and the MIPv6-related challenge and response messages are incorporated as additional data in the EAP protocol stack to enable Mobile IPv6 roaming in networks other than its home *(Faccin_Internet-Draft: page i, abstract)*.

- **Regarding claim 9**, Faccin '844 and Faccin_Internet-Draft disclose the method of claim 8.

Faccin_Internet-Draft further discloses MIPv6-related information is transferred in at least one EAP attribute in the EAP protocol stack *(Faccin_Internet-Draft: page 5, section 4.1; page 10, section 6.2; pages 22-24; sections 9.3-9.5)*.

- **Regarding claim 10**, Faccin '844 and Faccin_Internet-Draft disclose the method of claim 9.

Faccin_Internet-Draft further discloses the MIPv6- related information is transferred as EAP attributes of the method layer in the EAP protocol stack *(Faccin_Internet-Draft: page 5, section 4.1; page 10, section 6.2; pages 22-24; sections 9.3-9.5)*.

- **Regarding claim 12**, Faccin '844 and Faccin_Internet-Draft disclose the method of claim 9.

Faccin_Internet-Draft further discloses the MIPv6- related information is transferred in a generic container attribute available for any EAP method *(Faccin_Internet-Draft: pages 9-10; sections 6.1-6.3; the IPv6 mobile node should be able to use different authentication methods such as the different EAP types; the EAP data could be sent as an extension to ICMPv6 messages, carried using the protocol defined by the PANA EG or any other protocol)*.

- **Regarding claim 13**, Faccin '844 and Faccin_Internet-Draft disclose the method of claim 9.

Faccin_Internet-Draft further discloses the MIPv6- related information is transferred in a method-specific generic container attribute of the method layer in the EAP protocol stack *(Faccin_Internet-Draft: pages 9-10; sections 6.1-6.3; pages 14-15; section 7.5-7.6)*.

- **Regarding claim 14**, Faccin '844 discloses the method of claim 51.

Faccin '844 does not explicitly disclose the protocol for carrying authentication information for network access is selected from the group of the Protocol for carrying Authentication for Network Access (PANA), IEEE 802.1X, and Point-to-Point Protocol (PPP).

However, in an analogous art, Faccin_Internet-Draft discloses a Mobile IPv6 document, wherein the protocol for carrying authentication information for network access is selected from the group of the Protocol for carrying Authentication for Network Access (PANA), IEEE 802.1X, and Point-to-Point Protocol (PPP) *(Faccin_Internet-Draft: page 5, section 4.1; page 10, section 6.2; the EAP data could be sent as an extension to ICMPv6 messages, carried suing the protocol defined by the PANA WG or any other protocol)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Faccin_Internet-Draft with the method and system of Faccin wherein the protocol for carrying authentication information for network access is selected from the group of the Protocol for carrying Authentication for Network Access (PANA), IEEE 802.1X, and Point-to-Point Protocol (PPP) to enable Mobile IPv6 roaming in networks other than its home *(Faccin_Internet-Draft: page i, abstract)*.

- **Regarding claim 22**, Faccin '844 discloses the method of claim 19.

Faccin '844 does not explicitly disclose building, at the mobile node, a home address for the mobile node using at least a portion of the address of its assigned home agent; and transferring the home address of the mobile node from the mobile node to the AAA home network server using around trip of a selected EAP procedure.

However, in an analogous art, Faccin_Internet-Draft discloses a Mobile IPv6 document, including steps of building, at the mobile node, a home address for the mobile node using at least a portion of the address of its assigned home agent *(Faccin_Internet-Draft: page 12, section 7.3.1; pages 15-16, section 7.6; page 20-21, section 9.2.1)*; and transferring the home address of the mobile node from the mobile node to the AAA home network server using around trip of a selected EAP procedure *(Faccin_Internet-Draft: page 12, section 7.3.1; page 2-21, section 9.2.1)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Faccin_Internet-Draft with the method and system of Faccin to include steps of building, at the mobile node, a home address for the mobile node using at least a portion of the address of its assigned home agent; and transferring the home address of the mobile node from the mobile node to the AAA home network server using around trip of a selected EAP procedure to enable Mobile IPv6 roaming in networks other than its home *(Faccin_Internet-Draft: page i, abstract)*.

- **Regarding claims 31-33**, claims 31-33 are similar in scope to claims 8-10 respectively, and are therefore rejected under similar rationale.

- **Regarding claims 35-37**, claims 35-37 are similar in scope to claims 12-14 respectively, and are therefore rejected under similar rationale.

15. **Claims 11 and 34 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Faccin '844 and Faccin_Internet-Draft, as applied to claims 51 and 52 above, and further in view of Akhtar et al., (hereinafter "Akhtar"), U.S. Patent No. 7,079,499, filed on September 07, 2000.

- **Regarding claim 11**, Faccin '844 and Faccin_Internet-Draft disclose the method of claim 10.

Faccin '844 and Faccin_Internet-Draft do not explicitly disclose the EAP attributes are EAP Type-Length-Value (TLV) attributes.

However, in an analogous art, Akhtar discloses a mobility architecture framework, wherein the EAP attributes are EAP Type-Length-Value (TLV) attributes *(Akhtar: col. 88, lines 4-10)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Akhtar with the method and system of Faccin '844 and Faccin_Internet-Draft, wherein the EAP attributes are EAP Type-Length-Value (TLV) attributes to provide a communication architecture for enabling IP-based mobile communications *(Akhtar: col. 1, lines 56-58)*.

- **Regarding claim 34**, claim 34 is similar in scope to claim 11, and is therefore rejected under similar rationale.

16. **Claims 18 and 41 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Faccin '844, as applied to claims 51 and 52 above, in view of Akhtar et al., (hereinafter "Akhtar"), U.S. Patent No. 7,079,499, filed on September 07, 2000.

- **Regarding claim 18**, Faccin '844 discloses the method of claim 16.

Faccin '844 does not disclose the AAA framework protocol application is an application of a protocol selected from the group of Diameter and RADIUS.

However, in an analogous art, Akhtar discloses a mobility architecture framework, wherein the AAA framework protocol application is an application of a protocol selected from the group of Diameter and RADIUS *(Akhtar: col. 26, lines 1-7; col. 27, lines 1-5; col. 31, lines 36-42)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Akhtar with the method and system of Faccin '844, wherein the AAA framework protocol application is an application of a protocol selected from the group of Diameter and RADIUS to provide a communication architecture for enabling IP-based mobile communications *(Akhtar: col. 1, lines 56-58)*.

- **Regarding claim 41**, claim 41 is similar in scope to claim 18, and is therefore rejected under similar rationale.

Conclusion

17. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information

for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437